

*In the Specification:*

Please replace paragraph [0017] in the specification with the following new paragraph [0017]. Please replace paragraph [0019] in the specification with the following new paragraph [0019]. Please replace paragraph [0024] in the specification with the following new paragraph [0024]. The replacement paragraphs are presented with additions underlined and deletions in ~~strikethrough~~ text. No new matter is added by this amendment.

[0017] Sweatte, in U.S. Pat. No. 6,4335,688, describes a method and system for airport security using biometric data and a wireless smart card. Upon check-in a traveler must undergo identification by means of a fingerprint or retinal scan, provide a government issue ID card, such as a driver's license, and have his photograph taken. This information is verified against law enforcement databases and if the verifications return positively the traveler is supplied with a wireless smart card. The traveler is required to carry this smart card for the duration of travel within the airport and on-board the airplane, and it is used to track the individual's journey. However, the smart card is not tied to the individual by anything other than the issuing process; Therefore, an individual's card could be lost, stolen, discarded, or illegally transferred to another individual. The Sweatte patent does not address privacy issues or multiple different travel privileges.

[0019] The cognitive system for a vehicle and its occupants, as depicted by Gehlot in U.S. Pat. No. 6,310,2542, receives, processes, and stores real-time data gathered from the electronic subsystems of a motor vehicle. It also includes a data collection method for validating and authorizing an individual to the vehicle, thus restricting operators to an approved subset. This data assembly is performed by gathering biometric information from the driver and reading the information from a user-supplied 'vehicle information card'. The known credentials are stored within memory located in the vehicle and do not require a centralized database. However, as described in the patent, the system has a wireless link to the Department of Transportation and the Division of Motor Vehicles

("DMV") in order to report additional information to these agencies. Gehlot does not, however, detail how these credentials are initially verified and validated, and therefore cannot guarantee that the information enrolled in the car's memory is accurate. The Gehlot invention also does not prevent the information in the vehicle information card from being altered after issuance.

[0024] In U.S. Pat. No. 4,738,1334, Weishaupt teaches a security installation for motor vehicles that uses a stationary transponder attached to the vehicle and a portable transponder that is carried by a potential driver. The stationary transponder transmits a coded signal to the portable transponder; upon receipt of the coded signal the portable transponder transmits a coded response signal. If the stationary transponder receives a signal that it expects, it creates an unlocking signal to send to the vehicle's unlocking system. This system does not require that the potential driver authenticate himself to the portable transponder, so the driver of the vehicle cannot be identified.

Please insert the following two (2) new paragraphs in the specification between paragraph [0083] and the section entitled "DETAILED DESCRIPTION OF THE INVENTION."

Figure 7 illustrates components of a biometric personal identification device (BPID).

Figure 8 illustrates an exterior view of the BPID shown in Figure 7.

Please insert the following three (3) new paragraphs in the specification between paragraph [0112] and paragraph [0113].

FIGS. 7 and 8 illustrate the components of the BPID and an exterior view of the BPID, respectively, according to an embodiment of the invention. As shown in FIG. 7, the components of the BPID include a processor, a memory, a wireless transceiver, a fingerprint sensor and a battery. The components of the BPID can optionally include a

touch screen (e.g., a graphic liquid crystal display), a speaker and a GPS receiver. As shown in FIG. 8, the BPID can display a name, date of birth, birthplace, issue data and expiration date for a user of the BPID.

The user will undergo an enrollment process at an enrollment station to have his name, nationality, date of birth, location of birth, and other information downloaded to the BPID. The enrollment process also adds digital representations of the applicant's fingerprint, photograph and handwritten signature to the device. After enrollment the individual is able to authorize release of the information by authenticating his fingerprint to the BPID, digitally sign the data with his personal private key, and transmit the information via the wireless link. Furthermore, the BPID will have methods for receiving virtual 'stamps' at ports of entry.

The user authentication process is performed in a manner supportive of the individual's right to privacy. In one embodiment, a pre-enrolled biometric template of the authorized individual within tamper-resistant memory is stored within the BPID. The template is never authorized to leave the BPID, and is "zeroed-out" upon unauthorized attempted physical or logical access. When an individual wishes to access controlled resources, he/she submits another biometric template through a reader on the BPID. If the submitted identity credential matches the template stored therein, the user is granted access to operate the BPID and the machinery it controls.